METHOD AND DEVICE FOR MONITORING DATA TRAFFIC AND PREVENTING UNAUTHORIZED ACCESS TO A NETWORK

ABSTRACT OF THE DISCLOSURE

A method and device for protecting a network by monitoring both incoming and outgoing data traffic on multiple ports of the network, and preventing transmission of unauthorized data across the ports. The monitoring system is provided in a non-promiscuous mode and automatically denies access to data packets from a specific source if it is determined that the source is sending unauthorized data (e.g., suspicious data or a denial of service attack). All other packets from sources not transmitting unauthorized data are allowed to use the same port. The monitoring system processes copies of the data packets resulting in minimal loss of throughput. The system is also highly adaptable and provides dynamic writing and issuing of firewall rules based on sample time and a threshold value for the number of packets transmitted. Information regarding the data packets is captured, sorted and cataloged to determine attack profiles and unauthorized data packets.